UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/643,564	08/18/2003	Bruce McCorkendale	SYMC1032	4932

34350 7590 12/31/2007
GUNNISON, MCKAY & HODGSON, L.L.P.
1900 GARDEN ROAD, SUITE 220
MONTEREY, CA 93940

EXAMINER	
KHOSHNOODI, NADIA	
ART UNIT	PAPER NUMBER
2137	
MAIL DATE	DELIVERY MODE
12/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/643,564	**Applicant(s)** MCCORKENDALE ET AL.	
	Examiner Nadia Khoshnoodi	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 September 2007*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-11 and 15-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-11 and 15-28* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 August 2003* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 9/21/2007 has been entered.

Response to Amendment

Claims 2 and 12-14 are cancelled. Applicant's arguments/amendments with respect to amended claims 1, 15, 20, & 26 and previously presented claims 3-11, 16-19, 21-25, & 27-28 filed 8/30/2007 have been fully considered and are therefore rejected under new grounds.

Claim Objections

Claims 27-28 are objected to because of the following informalities: these claims should refer to "the computer readable medium configured to store computer program code further comprising..." instead of to "the computer program product of claim 26 further comprising…" since a computer program product is not the statutory class of invention being claimed in claim 26. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 4 and 27 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The term "recently" in claims 4 and 27 is a relative term which renders the claims indefinite. The term "recently" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

II. Claims 1, 3-7, and 26-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pak et al., US Patent No. 7,080,408 and further in view of Hoepers et al., "Honeynets Applied to the CSIRT Scenario."

As per claims 1 and 26:

Pak et al. substantially teach a method/computer program product comprising a computer readable medium configured to store code, the method/computer program product comprising:

comparing outbound traffic on a host computer system to inbound traffic on the host computer system, wherein the inbound traffic is received on the host computer system from a source external to the host computer system (col. 5, lines 3-28); and determining if malicious code is detected on the host computer system based on the comparing (col. 5, lines 28-30); when malicious code is detected, providing a notification of the malicious code detection (col. 7, line 4-12).

Not explicitly disclosed is wherein the outbound traffic is generated on the host computer system for transmission from the host computer system to a destination external to the host computer system. However, Hoepers et al. teach that outgoing traffic generated on a host machine which are not in response to an incoming packet received are captured and an alert for interception of malicious traffic is generated. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Pak et al. to compare the outgoing traffic to determine whether or not it is in response to incoming/received traffic in order to create an alert when the outgoing traffic is generated on the host machine is not in response to any of the received/incoming traffic. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Hoepers et al. suggest that generating an alert for outgoing traffic generated without being a response to incoming traffic will help lessen the impact that malicious traffic has on a network on page 5, section 2.4.1, number 1.

As per claim 3:

Pak et al. and Hoepers et al. substantially teach the method of claim 1. Furthermore, Pak et al. teach the method wherein the comparing is performed using a similarity comparison technique (col. 5, lines 15-33).

As per claim 4:

Pak et al. and Hoepers et al. substantially teach the method of claim 1. Furthermore, Pak et al. teach the method wherein at least a portion of the outbound traffic is compared to at least a recently received portion of the inbound traffic, the at least a portion of the outbound traffic being subsequent in time to the at least a recently received portion of the inbound traffic (col. 5, lines 15-33).

As per claim 5:

Pak et al. and Hoepers et al. substantially teach the method of claim 1. Furthermore, Hoepers et al. teach the method wherein the inbound traffic is received at the host computer system from a source port, and wherein the outbound traffic is for sending to a destination port, and further wherein the source port and the destination port are the same port (pg. 3, section 2.2.1).

As per claim 6:

Pak et al. and Hoepers et al. substantially teach the method of claim 1. Furthermore, Pak et al. teach the method wherein the inbound traffic is received on the host computer system from a source port, and wherein the outbound traffic is for sending to a destination port, and further wherein the source port and the destination port are different ports (col. 5, lines 20-28).

As per claim 7:

Pak et al. and Hoepers et al. substantially teach the method of claim 1. Furthermore, Pak et al. teach the method further comprising: implementing protective actions (col. 5, lines 39-47).

As per claim 27:

Pak et al. and Hoepers et al. substantially teach the computer program product of claim 26. Furthermore, Pak et al. teach the method wherein at least a portion of the outbound traffic is compared to at least a recently received portion of the inbound traffic, the at least a portion of the outbound traffic being subsequent in time to the at least a recently received portion of the inbound traffic (page 5, section 2.4.1, number 1). Further Pak et al. teach wherein the comparing is performed using a similarity comparison technique (col. 5, lines 15-33).

As per claim 28:

Pak et al. and Hoepers et al. substantially teach the computer program product of claim 26. Furthermore, Pak et al. teach the method further comprising: implementing protective actions (col. 5, lines 39-47).

III. Claims 15-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chesla et al., US Pub. No. 2004/0250124 further in view of Hoepers et al., "Honeynets Applied to the CSIRT Scenario.".

As per claim 15:

Chesla et al. substantially teach a method comprising: intercepting inbound traffic on a host computer system, wherein the inbound traffic is received on the host computer system from a source external to the host computer system (par. 121); copying the inbound traffic to an inbound traffic memory area, the copying the inbound traffic generating copied inbound traffic (par. 365-370); releasing the inbound traffic (par. 353-355); intercepting outbound traffic on the host computer system(par. 149); copying the outbound traffic to an outbound traffic memory area, the copying the outbound traffic generating copied outbound traffic (par. 300); releasing the outbound traffic (par. 353-355); comparing at least a portion of the copied inbound traffic with at least a portion of the copied outbound traffic (par. 137); determining if malicious code is detected on the host computer system based on the comparing (par. 137); and if malicious code is detected, providing a notification of the malicious code detection (par. 435).

Not explicitly disclosed is wherein the outbound traffic is generated on the host computer system for transmission from the host computer system to a destination external to the host computer system. However, Hoepers et al. teach that outgoing traffic generated on a host machine which are not in response to an incoming packet received are captured and an alert for interception of malicious traffic is generated. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Chesla et al. to compare the outgoing traffic to determine whether or not it is in response to incoming/received traffic in order to create an alert when the outgoing traffic is generated on the host machine is not in response to any of the received/incoming traffic. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Hoepers et al. suggest that generating an alert for outgoing traffic generated without being a response to incoming traffic will help lessen the impact that malicious traffic has on a network on page 5, section 2.4.1, number 1.

As per claim 16:

Chesla et al. and Hoepers et al. substantially teach the method of Claim 15. Furthermore, Chesla et al. teach wherein the comparing is performed using a similarity comparison technique (par. 159).

As per claim 17:

Chesla et al. and Hoepers et al. substantially teach the he method of claim 15. Furthermore, Chesla et al. teach wherein the at least a portion of the copied outbound traffic is subsequent in time to the at least a portion of the copied inbound traffic (par. 159).

As per claim 18:

Chesla et al. and Hoepers et al. substantially teach the method of claim 15. Furthermore, Chesla et al. teach the method further comprising: prior to the copying the outbound traffic, if the outbound traffic correlates to a prior name resolution lookup performed on the host computer system, releasing the outbound traffic (par. 134 and 289).

As per claim 19:

Chesla et al. and Hoepers et al. substantially teach the he method of claim 15. Furthermore, Chesla et al. teach wherein the inbound traffic is copied to the inbound traffic memory area on a per port basis (par. 189), and wherein the outbound traffic is copied to the outbound traffic memory area on a per destination port basis (par. 295).

As per claim 20:

Chesla et al. substantially teach a method comprising: intercepting inbound traffic on a host computer system, wherein the inbound traffic is received on the host computer system from a source external to the host computer system (par. 121); copying the inbound traffic to an inbound traffic memory area, the copying the inbound traffic generating copied inbound traffic (par. 264); releasing the inbound traffic (par. 353-355); intercepting outbound traffic on the host computer system(par. 149); buffering the outbound traffic in an outbound traffic memory area, the buffering the outbound traffic generating buffered outbound traffic (par. 149); comparing at least a portion of the copied inbound traffic with at least a portion of the buffered outbound traffic (par. 137 and 159); determining if malicious code is detected on the host computer system based on the comparing (par. 137); if malicious code is detected, providing a notification of the malicious code detection (par. 354); and if malicious code is not detected, releasing the at least a portion of the buffered outbound traffic (par. 160).

Not explicitly disclosed is wherein the outbound traffic is generated on the host computer system for transmission from the host computer system to a destination external to the host computer system. However, Hoepers et al. teach that outgoing traffic generated on a host machine which are not in response to an incoming packet received are captured and an alert for interception of malicious traffic is generated. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Chesla et al. to compare the outgoing traffic to determine whether or not it is in response to incoming/received traffic in order to create an alert when the outgoing traffic is generated on the host machine is not in response to any of the received/incoming traffic. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Hoepers et al. suggest that generating an alert for outgoing traffic generated without being a response to incoming traffic will help lessen the impact that malicious traffic has on a network on page 5, section 2.4.1, number 1.

As per claim 21:

Chesla et al. and Hoepers et al. substantially teach the method of claim 20. Furthermore, Chesla et al. teach wherein the comparing is performed using a similarity comparison technique (par. 159).

As per claim 22:

Chesla et al. and Hoepers et al. substantially teach the method of Claim 20. Furthermore, Chesla et al. teach wherein the at least a portion of the buffered outbound traffic is subsequent in time to the at least a portion of the copied inbound traffic (par. 159).

As per claim 23:

Chesla et al. and Hoepers et al. substantially teach the method of claim 20. Furthermore, Chesla et al. teach the method further comprising: prior to buffering the outbound traffic, if the outbound traffic correlates to a prior name resolution lookup performed on the host computer system, releasing the outbound traffic (par. 134 and 289).

As per claim 24:

Chesla et al. and Hoepers et al. substantially teach the method of claim 20. Furthermore, Chesla et al. teach wherein the inbound traffic is copied to the inbound traffic memory area on a per port basis (par. 189), and wherein the outbound traffic is buffered in the outbound traffic memory area on a per destination port basis (par. 295).

As per claim 25:

Chesla et al. and Hoepers et al. substantially teach the method of claim 20. Furthermore, Chesla et al. teach wherein if malicious code is detected, implementing protective actions (par. 134-135).

IV. Claims 8-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pak et al., US Patent No. 7,080,408 and Hoepers et al., "Honeynets Applied to the CSIRT Scenario," as applied to claim 1 above, and further in view of Chesla et al., US Pub. No. 2004/0250124.

As per claim 8:

Pak et al. and Hoepers et al. substantially teach the method of claim 1. Pak et al. further teaches that a message digest may be stored when the traffic is intercepted (col. 6, lines 4-19). Not explicitly disclosed is the method further comprising: intercepting the inbound traffic; copying the inbound traffic to an inbound traffic memory area, the copying the inbound traffic generating copied inbound traffic; releasing the inbound traffic; intercepting the outbound traffic; copying the outbound traffic to an outbound traffic memory area, the copying the outbound traffic generating copied outbound traffic; and releasing the outbound traffic. However, Chesla et al. teach that copies of values of the incoming traffic/outgoing traffic may be stored in both inbound and outbound directions in order to allow for detecting possible attacks. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Pak et al. and Hoepers et al. to store a copy of the inbound and outbound traffic in different memory areas in order to determine if a possible flooding attack (as one example) is underway. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Chesla et al. suggest that using a list of incoming/outgoing signatures and monitoring that list closely (while still releasing the traffic) provides a great technique for various attack detections on a network in par. 353-355.

As per claim 9:

Pak et al., Hoepers et al., and Chesla et al. substantially teach the method of claim 8. Furthermore, Chesla et al. teach wherein the comparing comprises: comparing at least a portion of the copied inbound traffic with at least a portion of the copied outbound traffic.

As per claim I0:

Pak et al. and Hoepers et al. substantially teach the method of claim 1. Not explicitly disclosed is the method further comprising: intercepting the inbound traffic; copying the inbound traffic to an inbound traffic memory area, the copying the inbound traffic generating copied inbound traffic; releasing the inbound traffic; intercepting the outbound traffic; buffering the outbound traffic in an outbound traffic memory area, the buffering the outbound traffic generating buffered outbound traffic; and if malicious code is not detected releasing the buffered outbound traffic. However, Chesla et al. teach that copies of values of the incoming traffic/outgoing traffic may be stored in both inbound and outbound directions in order to allow for detecting possible attacks. Furthermore, Chesla et al. teach wherein buffering techniques may be used on outgoing traffic to lower the rate at which the traffic can continue on to its final destination. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Pak et al. and Hoepers et al. to store a copy of the inbound and outbound traffic in different memory areas in order to determine if a possible flooding attack (as one example) is underway, as well as to buffer the outgoing traffic. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Chesla et al. suggest that using a list of incoming/outgoing signatures and monitoring that list closely (while still releasing the traffic) provides a great technique for various attack detections on a network in par. 353-355.

Furthermore, Chesla et al. suggest that buffering the traffic can lessen the impact of an attack, since by buffering the outgoing traffic the system allows for lowering the rate at which the traffic can proceed in par. 149.

As per claim 11:

Pak et al., Hoepers et al., and Chesla et al. substantially teach the method of claim 10. Furthermore, Chesla et al. teach wherein the comparing comprises: comparing at least a portion of the copied inbound traffic with at least a portion of the buffered outbound traffic (par. 149).

**References Cited, Not Used*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. US Pub. No. 2003/0154255
2. US Pub. No. 2006/0212572
3. US Pub. No. 2003/0074578
4. US Patent No. 6,925,572
5. US Pub. No. 2004/0111531
6. US Pub. No. 2003/0101353

The above references have been cited because they are relevant due to the manner in which the invention has been claimed.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Nadia Khoshnoodi

Nadia Khoshnoodi
Examiner
Art Unit 2137
12/26/2007

NK

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER